DDSGA: A Data-Driven Semi-Global AlignmentApproach for Detecting Masquerade Attacks

A masquerade attacker impersonates a legal user to utilize the user services and privileges. The semi-global alignmentalgorithm (SGA) is one of the most effective and efficient techniques to detect these attacks but it has not reached yet the accuracy andperformance required by large scale, multiuser systems. To improve both the effectiveness and the performances of this algorithm, wepropose the Data-Driven Semi-Global Alignment, DDSGA approach. From the security effectiveness view point, DDSGA improves thescoring systems by adopting distinct alignment parameters for each user. Furthermore, it tolerates small mutations in user commandsequences by allowing small changes in the low-level representation of the commands functionality. It also adapts to changes in theuser behaviour by updating the signature of a user according to its current behaviour. To optimize the runtime overhead, DDSGAminimizes the alignment overhead and parallelizes the detection and the update. After describing the DDSGA phases, we present theexperimental results that show that DDSGA achieves a high hit ratio of 88.4 percent with a low false positive rate of 1.7 percent. Itimproves the hit ratio of the enhanced SGA by about 21.9 percent and reduces Maxion-Townsend cost by 22.5 percent. Hence,DDSGA results in improving both the hit ratio and false positive rates with an acceptable computational overhead.

EXISTING SYSTEM:

1. Semi-global alignment (SGA) is one of the most efficient detection algorithms and its accuracy was improved by Coull et al.
2. Naïve Bayes One-step Markov is based upon one-step transitions from a command to the next. It builds two transition matrices for each user from, respectively, the training database and the testing one and it triggers an alarm when these matrices noticeably differ.
3. Schonlau et al. toggled between a Markov model and the simple independence one.
4. Dash et al. introduced an episode based Na€ive Bayes technique that extracts meaningful episodes from a long sequence of commands.

DISADVANTAGES OF EXISTING SYSTEM:

1. The current detection approaches have not achieved the level of accuracy and performance for practical deployment in spite of the large amount of information they used to build a profile such as command line commands, system calls, mouse movements, opened files names, opened windows title, and network actions.
2. While uniqueness has a relatively poor performance, it is one of the few approaches that target false alarm rate of 1 percent.
3. The false alarm rate of this method is not satisfactory.

PROPOSED SYSTEM:

1. This paper introduces the Data-Driven Semi-Global Alignment (DDSGA) approach, which improves both the detection accuracy and the computational performance of the Enhanced-SGA and of HSGAA that is also based upon SGA.
2. The main idea underlying DDSGA is to consider the best alignment of the active session sequence to the recorded sequences of the same user. After discovering the misalignment areas, we label them as anomalous and several anomalous areas are a strong indicator of a masquerade attack.
3. DDSGA can tolerate small mutations in the user sequences with small changes in the low level representation of user commands and it is decomposed into a configurationphase, a detection phase and an update one.
4. The configuration phase, computes, for each user, the alignment parameters to be used by both the detection andupdate phases.
5. The detection phase aligns the user current session to the signature sequence. The computational performance of this phase is improved by two approaches namely the Top-Matching Based Overlapping (TMBO) andthe parallelized approach.
6. In the update phase, DDSGA extends both the user signatures and user lexicon list withthe new patterns to reconfigure the system parameters.

ADVANTAGES OF PROPOSED SYSTEM:

1. DDSGA improves the security efficiency by using not only lexical matching such as string matching or longest common substring searches, but also by tolerating small mutations in the sequences with small changes in the low-level representation of the user commands.
2. To increase the hit ratio and reduce both false positive and false negative rates, DDSGA pairs each user with distinct gap insertion penalties according to the user behavior.
3. Furthermore, it improves both the alignment scoring system and the update phase of Enhanced-SGA to tolerate changes in behaviours without significantly reducing the alignment score.
4. DDSGA improves both the computational and the securityefficiency of the Enhanced-SGA.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

1. System : Pentium IV 2.4 GHz.
2. Hard Disk : 40 GB.
3. Floppy Drive : 1.44 Mb.
4. Monitor : 15 VGA Colour.
5. Mouse : Logitech.
6. Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

Operating system	:	Windows XP/7.
Coding Language	:	JAVA(AWT,Swings,Networking)
IDE	:	Eclipse Galileo
Database	:	MS Access/MYSQL